

OFFICER'S CPNI COMPLIANCE CERTIFICATE

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011.

Date filed: February 21, 2012

Name of company covered for this certification: Atwood Cable Systems, Inc.

Form 499 Filer ID: 827185

Name of signatory: Robert J. Dunker

Title of signatory: Vice President

I, Robert J. Dunker, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Robert J. Dunker

[electronic signature]

## ATTACHMENT

### ATWOOD CABLE SYSTEMS, INC. STATEMENT OF CPNI OPERATING PROCEDURES

1. It is the policy of Atwood Cable Systems, Inc. ("ACSI") not to use, disclose, or permit access to Customer Proprietary Network Information ("CPNI"), as defined in the FCC's rules, for any purposes other than the following, all of which are permitted without customer approval under FCC rules:
  - a. For the purpose of providing or marketing ACSI service offerings among categories of service (i.e., local, interexchange) to which the customer already subscribes.
  - b. For the purpose of providing inside wiring installation, maintenance, and repair services.
  - c. For the purpose of marketing "adjunct-to-basic" services, such as speed dialing, call monitoring, call blocking, call return, repeat dialing, voice mail, call waiting, caller I.D., call forwarding, and certain centrex features.
  - d. For the purpose of protecting the rights or property of ACSI, or to protect users of its services and other carriers from fraud, abusive, or unlawful use of or subscription to such services.
2. ACSI established a program to inform and train personnel that they may not use, disclose, or permit access to CPNI for any purpose other than those set forth above. At present, the Company does not engage in outbound marketing using CPNI. The Company has an express disciplinary process in place to discipline violations of its CPNI policy.
3. Because ACSI does not use, disclose or permit access to CPNI except as described above, by definition, it does not need to maintain a record of sales and marketing campaigns that use

customers? CPNI or of instances where CPNI is disclosed to third parties, or where third parties were allowed access to CPNI.

4. Because ACSI does not use CPNI except as described above, ACSI does not utilize a notification and customer approval process (i.e., an opt-out or opt-in process). If the Company changes its marketing procedures, an appropriate customer notification process will be instituted.

5. ACSI offers to customers, online access to customer phone features, voicemail and call detail. ACSI has measures to secure the customer information with proper authentication, including the use of passwords and other methods that comply with FCC rules to protect CPNI. ACSI will notify the customer immediately if the customer?s password is changed. This notification is made by mail, sent to the customer?s pre-existing address of record, and does not reveal the changed information.

6. Customers who contact ACSI via inbound calls are not able to access their call detail information. If in the future ACSI decides to convey call detail information to customers seeking such information via inbound calling, then ACSI will take measures to secure the customer information with proper authentication, including the use of passwords and other methods that comply with FCC rules to protect call detail information.

7. Customers who present themselves at ACSI?s retail location and who request CPNI are asked for proper photographic identification (i.e., state issued driver?s license or the equivalent.) CPNI will be disclosed only if the customer presents valid photo ID matching the customer?s account information.

8. ACSI has not detected any unauthorized access to CPNI, either by employees, pretexters or other third parties. ACSI did not receive any customer complaints regarding CPNI in 2011.

9. ACSI will notify the customer immediately if the customer?s address of record is created (except at the time of service initiation) or changed. This notification is made by mail To the customer?s pre-existing address of record, and does not reveal the changed information.

10. In the event of any breach of a customer?s CPNI as described in section 64.2011 of the FCC rules, ACSI will, as soon as practicable and in all events within seven (7) days of determination of the breach, notify law enforcement through <http://www.fcc.gov/eb/cpni>, and subsequently notify the

customer(s), in accordance with the procedures and in the sequence prescribed by that rule section. ACSI will maintain a record of any such breaches and notifications for at least two (2) years.

11. ACSI has in place a supervisory review process regarding compliance with its CPNI policy.

12. ACSI has CPNI and Privacy policies available in its Public File, located at our office, and also available on ACSI website.